Getting your container(s) in to Iron Bank

What does success look like?

This checklist is meant to provide a high level overview of the process and steps for getting your container(s) in the Iron Bank

Getting Started

- [ ] **Create a Repo1 account to get access to the repository of containers**
  You can register by clicking on the 'Sign in with Iron Bank SSO' button in the sign-in page, followed by the Register button
- [ ] **Fill out the onboarding form.**
- [ ] **Attend our once weekly onboarding session where you can ask questions.**
  These sessions are every Wednesday from 1530-1630 EST. Reigster **here**.
- [ ] **Your Onboarding form will be processed by the Iron Bank team, who will then assign it a priority level and create your repository. You will receive an email that your Gitlab issue has been created and is ready for you to complete the hardening process**
- [ ] **Ensure that all POCs are assigned to the issue to ensure proper tracking and notifications**

Hardening Process

Repository Requirments

Full Documentation

- [ ] **A Dockerfile has been created in the root of the repository**

- [ ] Hardening_manifest.yaml has been created in the root of the repository
- [ ] The project has a LICENSE or a copy of the EULA
- [ ] The project has a README in the root of the repository with sufficient instructions on using the Iron Bank version of the image
- [ ] If your container is an enterprise/commercial container, the opensource version is ready
- [ ] Scripts used in the Dockerfile are placed into a `scripts` directory
- [ ] Configuration files are placed into a `config` directory
- [ ] Project is configured for automatic renovate updates (if possible)
  - [ ] Renovate.json is present in root of repository
  - [ ] Reviewers have been specified for notifications on new merge requests

Dockerfile Requirements

Full Documentation

- [ ] There is one Dockerfile named Dockerfile

- [ ] The Dockerfile has the BASE_REGISTRY, BASE_IMAGE, and BASE_TAG arguments (used for local builds; the values in hardening_manifest.yaml are what will be used in the Container Hardening Pipeline)
- [ ] The Dockerfile is based on a hardened Iron Bank image
- [ ] The Dockerfile includes a HEALTHCHECK (required if it is an application container)
- [ ] The Dockerfile starts the container as a non-root USER. Otherwise, if you must run as root, you must have proper justification.
- [ ] If your ENTRYPOINT entails using a script, the script is copied from a scripts directory on the project root
- [ ] No ADD instructions are used in the Dockerfile

Hardening Manifest

Full Documentation

- [ ] Begin with this example and update with relevant information
- [ ] Hardening manifest adheres to the following schema
- [ ] The BASE_IMAGE and BASE_TAG arguments refer to a hardened/approved Iron Bank image (BASE_REGISTRY defaults to `registry1.dso.mil/ironbank` in the pipeline)

- [ ] Relevant image metadata has been entered for the corresponding labels
- [ ] Any downloaded resources include a checksum for verification (letters must be lowercase)
- [ ] For resource URLs that require authentication, credentials have been provided to an Iron Bank team member
- [ ] The maintainers' contact information has been provided in the `maintainers` section

Gitlab CI Pipeline

Full Documentation

- [ ] Validate your container builds successfully through the Gitlab CI pipeline. When viewing the repository in repo1.dso.mil, go to `CI/CD > Pipelines` on the left. From there, you can see the status of your pipelines.
- [ ] Review scan output from `csv output` stage of the pipeline. For instructions on downloading the findings spreadsheet, click here
- [ ] Fix vulnerabilities that were found and run the pipeline again before requesting a merge to the development branch

Pre-Approval

Full Documentation

- [ ] Submit a Merge Request to the development branch

- [ ] Feature branch has been merged into development
- [ ] All findings from the development branch pipeline have been justified per the above documentation
- [ ] Justifications have been attached to this issue
- [ ] Apply the `Approval` label and remove the `Doing` label to indicate this container is ready for the approval phase

Note: The justifications must be provided in a timely fashion. Failure to do so could result in new findings being identified which may start this process over.

Approval Process (Container Hardening Team processes):

Full Documentation

- [ ] Peer review from Container Hardening Team
- [ ] Findings Approver has reviewed and approved all justifications
- [ ] Approval request has been sent to Authorizing Official
- [ ] Approval request has been processed by Authorizing Official

One of the following statuses is assigned:

- [ ] Conditional approval has been granted by the Authorizing Official for this container (`Approval::Expiring` label is applied)
- [ ] This container has been approved by the Authorizing Official (`Approved` label is applied)

Post-Approval

Full Documentation

- [ ] Your issue has been closed
- [ ] Your project has been merged into master
- [ ] Master branch pipeline has completed successfully (at this point, the image is made available on `ironbank.dso.mil` and `registry1.dso.mil`)

Note: Now that your application has been approved, your container(s) will be subjected to continuous monitoring. If new CVEs are discovered or bugs are identified, you will need to address the issues and return to step 5 (Gitlab CI Pipeline). As you make changes, please make sure you are adhering to all of the requirements of the hardening process.